UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/755,470	01/05/2001	Steven Branigan		4994

27997 7590 04/13/2007
PRIEST & GOLDSTEIN PLLC
5015 SOUTHPARK DRIVE
SUITE 230
DURHAM, NC 27713-7736

EXAMINER	
TRAN, ELLEN C	
ART UNIT	PAPER NUMBER
2134	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/13/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	**Application No.** 09/755,470	**Applicant(s)** BRANIGAN ET AL.	
	Examiner Ellen C. Tran	**Art Unit** 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _29 January 2007_.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-15_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-15_ is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. This action is responsive to: amendment filed 29 January 2007 with acknowledgement of an original application filed on 05 January 2001 and acknowledgement of priority established by affidavit to 22 February 2000 and further declared in arguments to 05 January 2000.

2. Claims 1-15 are currently pending in this application. Claims 1, 7, and 10 are independent claims. Claims 1, 7, and 10 have been amended, amendment to the claims is accepted.

Claim Objections

3. Claim 7 is objected to because of the following informalities: "a wireless network clients" is stated in the amended claims, it should indicate "client". Appropriate correction is required.

Response to Arguments

4. Applicant's arguments filed 29 January 2007 have been fully considered however they are moot due to the new grounds of rejection below initiated by amendment to all the independent claims.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. **Claims 1 and 7,** are rejected under 35 U.S.C. 103(a) as being unpatentable over Massarani US Patent No. 6,393,484 (hereinafter '484) in view of Lewis US Patent No. 6,526,506 (hereinafter '506).

As to independent claim 1, "A wired network for providing secure, authenticated access to wireless network clients, comprising: a server connected to a wireless network access point, and having access to the wired network, the server being operative to perform authentication for a wireless client" is taught in '484 col. 4, lines 31-66;

"establishing a connection to the server through the wireless network access point, the server performing authentication by examining authentication information transmitted from the client to the server" is disclosed in '484 col. 5, lines 7-25;

"and determining whether or not the authentication information identifies the wireless network client as authorized to gain access to the wired network, the server being operative to establish a connection session upon authentication of a client, the server being also operative to provide the client with a wired network address valid for the connection session upon authentication of the client," is taught in '484 col. 4, lines 31-41 and also see col. 6, lines 23-53;

"and a user database accessible to the server for use in validating wireless clients" is shown in '484 col. 5, lines 8-19;

the following is not explicitly taught in '484:

"the server being further operative to encrypt communications with the wireless network access point, the server being further operative to provide a cryptographic key to the client to be used for encrypted communication with the wired network and valid for the

connection session upon authentication of the client" however '506 teaches "the key distribution server 76 responds to the encrypted request packet with a response packet containing the ENCRYPT key in its data field as is discussed below in relation to FIG. 8. The processor 142 passes the response packet through the encryption engine 146 in order to encrypt the response packet using the MASTER key. The response packet is addressed to the mobile terminal 66 requesting the ENCRYPT key, and is transmitted out onto the system backbone 52. The access point 54 with which the mobile terminal 66 is registered will detect and receive the response packet by detecting the network address of the mobile terminal in the destination address of the non-encrypted header field. The access points 54, in the preferred embodiment, are also configured to detect from the header field when a packet originates from the key distribution server 76 (as noted from the source address of the header field). In the event a packet originates from the key distribution server 76 as in the case of an ENCRYPT key response packet, the access points 54 are configured not to encrypt the packet via the ENCRYPT key and the encryption engine 118. Rather, the packet is simply forwarded to the destination mobile terminal 66 without encryption via the ENCRYPT key as discussed below in relation to FIG. 9. However, this will not jeopardize system security as will be appreciated since the response packet containing the ENCRYPT key already has been encrypted using the MASTER key by the key distribution server 76. Thus, the mobile terminal 66 may still be informed of the ENCRYPT key via the wireless link without jeopardizing system security" in col. 11, line 64 through col. 12, line 26. Note as explained the response to the client (i.e. mobile terminal) is encrypted with the client's MASTER key, this is the encrypted communications exchanged with the AP then forwarded to the client, that contains the cryptographic key valid for the session (the ENCRYPT key).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify a system and method for providing network access to wireless clients via a server taught in '484 to include a means to provide secure wireless communication. One of ordinary skill in the art would have been motivated to perform such a modification to provide secure communications without the risk of compromise, see '506 (col. 2 lines 33 et seq.). "In view of the aforementioned shortcomings associated with existing wireless networks, there exists a strong need in the art for a wireless network which permits secure communications without substantial risk of compromise. In particular, there is a strong need for a wireless network which enables secure communications among mobile terminals capable of engaging in secure communications. At the same time, there is a strong need for a wireless network which is still capable of permitting communications by authorized mobile terminals requiring a non-secure format".

As to independent 7, "A wireless network for providing secure authenticated communication between clients of the wireless network and a wired network, comprising:" is taught in '484 col. 4, lines 31-66;

"a wireless network access point operative to establish a connection with a server operating as a portal between the wireless network and a wired network the wireless network access point being operative to conduct communications with the server in order to authenticate wireless network clients as authorized to access the wired network" is disclosed in '484 col. 5, lines 60-65;

"the wireless network access point being further operative to receive authentication information from one or more wireless network clients and transfer the authentication information to the server in order to allow the server to examine the authentication information for a wireless network client and determine if the information indicates that the wireless network client is authorized to access the wired network" is taught in '484 col. 6, lines 23-53;

"to pass authentication information to the network access point in order to indicate to a server communicating with the wireless network and a wired network whether or not the wireless client is authorized to gain access to the wired network, the wireless network client being further operative to and receive address information" is disclosed in '484 col. 6, lines 23-53;

the following is not explicitly taught in '484:

"the wireless network access point being operative to receive a cryptoprocessing key valid for a connection session from the server upon authentication of a client and to transfer the cryptoprocessing key to that client and a wireless network clients operative to establish connections with the wireless network access point, the client being operative to conduct encrypted communications with the server through the access point" and **"and the cryptoprocessing data from the network access point upon authentication by the server in order to allow communication with the wired network the client utilizingthe cryptoprocessing key to conduct encrypted transfer of data to and from the wired network through the access point upon receiving the address and the cryptoprocessing key"** however '506 teaches "the key distribution server 76 responds to the encrypted request packet with a response packet containing the ENCRYPT key in its data field as is discussed below in relation to FIG. 8. The processor 142 passes the response packet through the encryption engine 146 in order to encrypt the response packet using the MASTER key. The response packet is addressed to the mobile terminal 66 requesting the ENCRYPT key, and is transmitted out onto the system backbone 52. The access point 54 with which the mobile terminal 66 is registered will detect and receive the response packet by detecting the network address of the mobile terminal in the destination address of the non-encrypted header field. The access points 54, in the preferred embodiment, are also configured to detect from the header field when a packet originates from the key distribution server 76 (as noted from the source address of the header field). In the event a packet originates from the key distribution server 76 as in the case of an ENCRYPT key response packet, the access points 54 are configured not to encrypt the packet via the ENCRYPT key and the encryption engine 118. Rather, the packet is simply forwarded to the destination mobile terminal 66 without encryption via the ENCRYPT key as discussed below in relation to FIG. 9. However, this will not jeopardize system security as will be appreciated since the response packet containing the ENCRYPT key already has been encrypted using the MASTER key by the key distribution server 76. Thus, the mobile terminal 66 may still be informed of the ENCRYPT key via the wireless link without jeopardizing system security" in col. 11, line 64 through col. 12, line 26. Note as explained the response to the client (i.e. mobile terminal) is encrypted with the client's MASTER key, this is the encrypted communications exchanged with the AP then forwarded to the client, that contains the cryptographic key valid for the session (the ENCRYPT key).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify a system and method for providing network access to wireless clients via a server taught in '484 to include a means to provide secure wireless communication. One of ordinary skill in the art would have been motivated to perform such a modification to provide secure communications without the risk of compromise, see '506 (col. 2 lines 33 et seq.). "In view of the aforementioned shortcomings associated with existing wireless networks, there exists a strong need in the art for a wireless network which permits secure communications without substantial risk of compromise. In particular, there is a strong need for a wireless network which enables secure communications among mobile terminals capable of engaging in secure communications. At the same time, there is a strong need for a wireless network which is still capable of permitting communications by authorized mobile terminals requiring a non-secure format".

7. **Claims 2-5, 8-13,** are rejected under 35 U.S.C. 103(a) as being unpatentable over Massarani US Patent No. 6,393,484 (hereinafter '484) in view of Lewis US Patent No. 6,526,506 (hereinafter '506) in further view of Bhagwat et al. US Patent No. 6,651,105 (hereinafter '105).

As to independent 10, "A method of secure communication between wireless network clients and a wired network, comprising the steps of: establishing a connection between a wireless network access point and a security base (SB) server connected to the wired network; establishing a connection between the SB server and a wireless network client communicating with the SB server through the wireless network access point" is taught in '484 col. 4, lines 31-66;

"transmitting authentication information from the wireless network client to the SB server through the wireless network access point; performing authentication for the wireless network client by examining the authentication information to determine if the wireless network client is authorized to gain access to the wired network if authentication

fails, rejecting connection to the wired network and if authentication passes, accepting connection to the wired network, providing a temporary wired network address" is taught in '484 col. 6, lines 23-53;

the following is not explicitly taught in '484:

"exchanging encryption keys between the SB server and the wireless network client" however '506 teaches the server provides the ENCRYPT key to the mobile terminal, this key is used in the wireless communication session in col. 11, line 64 through col. 12, line 26;

"and a unique session encryption key to the wireless network client for encrypted communication with the wired network and valid for the connection session" however '506 teaches the ENCRYPT key provided is used for encrypted communication with the designated Access point in col. 11, line 64 through col. 12, line 26;

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify a system and method for providing network access to wireless clients via a server taught in '484 to include a means to provide secure wireless communication. One of ordinary skill in the art would have been motivated to perform such a modification to provide secure communications without the risk of compromise, see '506 (col. 2 lines 33 et seq.). "In view of the aforementioned shortcomings associated with existing wireless networks, there exists a strong need in the art for a wireless network which permits secure communications without substantial risk of compromise. In particular, there is a strong need for a wireless network which enables secure communications among mobile terminals capable of engaging in secure communications. At the same time, there is a strong need for a wireless network which is still capable of permitting communications by authorized mobile terminals requiring a non-secure format".

the following is not explicitly taught in '484 and '506:

"and providing access to wired network resources in response to requests by the wireless network client" however '105 teaches in col. 3, lines 41-48, note additional resources is an obvious variation of peers.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify a system and method for providing network access to wireless clients via a server taught in '484 and '506 to include a means to provide point to point security. One of ordinary skill in the art would have been motivated to perform such a modification to provide seamless access and security to the mobile user, see '105 (col. 1 lines 61 et seq. and col. 2, line 38 through col. 3, line 26). "It would be advantageous to have-a way which provides a seamless, secure mobility protocol for this kind of scenario ... A mobile host has a permanent home IP address which does not change upon movement to a new subnet. When a mobile host moves to a new subnet other than its home subnet, it registers its current location--the IP address of a foreign agent in the new subnet or a temporary IP address obtained by mechanisms such as DHCP- with an agent in its home subnet, called home agent ... The authentication is based on a shared secret key that can be manually configured in a mobile device and its home agent ... Since the range of the wireless link is short, these operations may need to be repeated quite frequently (with each hand-off to a new access point) ... Such a solution has the following drawbacks: A new PPP connection needs to be established with every hand-off. PPP connection establishment includes link configuration, authentication, network layer configuration, and optional encryption and compression parameter negotiations. Each parameter negotiation phase increases hand-off latency which may be unacceptable in micro-cellular, indoor wireless environments. Additionally, these negotiations waste bandwidth by introducing extra traffic on the wireless link. Layering Mobile IP on top of PPP adds to handoff latency because Mobile IP layer performs its own set of registration and authentication exchanges. This solution is difficult to deploy since Mobile IP protocol is not supported on most mobile devices".

As to dependent claim 11, "and wherein the step of accepting the connection is accompanied by a step of logging the acceptance" is taught in '484 col. 5, lines 17-19;

"wherein the step of rejecting connection to the wired network is accompanied by a step of logging the rejection" is shown in '484 col. 6, lines 11-23.

As to dependent 12, "wherein the step of providing a temporary wired network address to the wireless network client includes using dynamic host control protocol to provide the address" " is disclosed in '484 col. 3, lines 47-50.

As to dependent claim 2, "also including a network hub providing connections between the server" is taught in '484 FIG. 1 the edge router switch inherently is the network hub;

"and additional resources on the wired network" however '105 teaches in col. 3, lines 41-48, note additional resources is an obvious variation of peers. The motivation to combine '484, '506, and '105 is the same as stated above in claim 10.

As to dependent 3, "also including a router providing connections between the server" is taught in '484 col. 4, lines 54-67;

"and additional resources on the wired network" however '105 teaches in col. 3, lines 41-48, note additional resources is an obvious variation of peers.

"as well as a connection to an additional wired network" is shown in '484 col. 5, lines 55-65. The motivation to combine '105 and '484 is the as stated above in claim 10.

As to dependent 4, "wherein the server is operative to provide addresses to clients through dynamic host control protocol" is disclosed in '484 col. 3, lines 47-50.

As to dependent 5, "wherein the server is operative to communicate with a wireless network client using point to point tunneling protocol" however '105 teaches PPP is used for communications between the server and the wireless client in col. 4, lines 36-54. The motivation to combine '105 and '484 is the as stated above in claim 10.

As to dependent 8, "wherein the access point communicates with the server using point to point tunneling protocol" however '105 teaches PPP is used for communications between the server and the wireless client in col. 4, lines 36-54. The motivation to combine '105 and '484 is the as stated above in claim 10.

As to dependent 9, "including a hub connecting the wireless network access point and a plurality of additional network access points, each additional network access point communicating with a plurality of additional wireless network clients, the wireless network access point and- the additional network access points being operative to establish connections with the server through the network hub" is shown in '484 col. 4, lines 54-65.

As to dependent 13, "wherein communication between the wireless network client and the wired network server is performed using point to point tunneling protocol" however '105 teaches PPP is used for communications between the server and the wireless client in col. 4, lines 36-54. The motivation to combine '105, '506 and '484 is the as stated above in claim 10.

6. **Claim 6** is rejected under 35 U.S.C. 103(a) as being unpatentable over Massarani US Patent No. 6,393,484 (hereinafter '484) in view of Lewis US Patent No. 6,526,506 (hereinafter '506) in further view of Bhagwat et al. US Patent No. 6,651,105 (hereinafter '105) in further view of Redlich US Patent No. 6,591,306 (hereinafter '306).

As to dependent 6, the following is not explicitly taught in the combination of '105, '506, and '484: **"wherein the server employs 128-bit crypto-processing to communicate with the wireless network client"** however '306 teaches a 128 bit encryption key can be utilized in communication in col. 25, lines 43-67.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify a system and method for providing secure network access to wireless clients via a server taught in '484, '506, and '105 to include a means to utilize various encryption methods. One of ordinary skill in the art would have been motivated to perform such a modification to protect guest and host equipment and allow ease of use in a mobile network see '306 (col. 1 lines 21 et seq.). "It is therefore an object of the invention to solve the problem of hosting a guest station in a manner in which the guest simply plugs the guest station into the foreign network and gains instant IP connectivity. Another object is to achieve this even when the foreign network uses a broadcast LAN such as an Ethernet. Yet another object of the invention is to achieve the foregoing without change to the previously set network configuration of the portable device, including IP address, netmask, next-hop-routers (gateways) as well as settings for the Domain Name Service (DNS). It is a further object of the invention to achieve instant IP connectivity in a manner which prevents malicious attacks to the hosting network by the guest station. An additional object of the invention is to achieve the foregoing connectivity in a manner which permits the guest station, if desired, to provide for security against malicious intrusion or attacks from the foreign network. Furthermore, it is also an object of the invention to provide for IP access for a guest station without the need for a large pool of IP addresses. Finally, it is an important object of the invention to provide for IP access for a guest station without support from the guest station and without expecting support from the guest's regular network".

7. **Claim 14 and 15,** are rejected under 35 U.S.C. 103(a) as being unpatentable over Massarani US Patent No. 6,393,484 (hereinafter '484) in view of Lewis US Patent No. 6,526,506 (hereinafter '506) in further view of Bhagwat et al. US Patent.No. 6,651,105 (hereinafter '105) in further view of Schuster et al. U.S. Patent No. 6,857,072 (hereinafter '072).

As to dependent 14, "wherein the step of performing authentication for the wireless network client includes transferring authentication information between the wireless network client and the SB server" is taught in '484 col. 6, lines 23-53;

"and wherein the authentication information is encrypted" however '105 teaches 'Point-to-point protocol (PPP) is used for communication for wireless devices via access points. This communication can be encrypted if required' in col. 4, lines 36-54 and also col. 2, lines 20-24. The motivation to combine '484 and '105 is the same as stated above in claim 10 the following is not explicitly taught in the combination of '484, '506, and '105: **"using public key cryptography"** however '072 teaches the use of a public key to encrypt data transmitted over a network in col. 6, lines 44-64.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify a system and method for providing secure network access to wireless clients via a server taught in '484, '506, and '105 to include a means to utilize a public/private key encryption mechanism. One of ordinary skill in the art would have been motivated to perform such a modification so that sensitive data may be transmitted more securely see '072 (col. 3, lines 30 et seq.). "The present invention addresses the above needs by providing a system in a data network telephony system, such as for example, the Internet, that enables encryption and/or authentication on the telephony system. Users may participate in transactions with each other using more secure data channels. Sensitive data may be transmitted more safely across public networks".

As to dependent 15, "wherein the step of providing a unique session encryption key includes encrypting the unique session encryption key using public key cryptography" however '072 teaches the use of a public key to encrypt data transmitted over a network in col. 6, lines 44-64. The motivation to combine '484, '506, '105, and '072 is the same a stated above in claim 14.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a). A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 6:00 am to 4:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ECT

Ellen Tran
Patent Examiner
Technology Center 2134
10 April 2007

David Y. Jung
Primary Examiner

David Y. Jung
Primary Examiner